Implementation Plan for the Department of Commerce Significant Incident Coordination and Communication Process

The following process (pages 2 through 4) reflects the ideal steps for a smooth and orchestrated flow of activities and communications surrounding computer security events of concern to the federal government. Occasionally, the Department must respond to external data calls regarding the Department's security posture in light of significant computer security events such as the recent SQL Slammer Worm. A "Significant Event" is one which the Federal Computer Incident Response Center (FedCIRC) and the Office of Management and Budget (OMB) have determined to be of significant impact to the federal government.

Currently, DOC IT Security Program Policy requires that all operating units have in place mechanisms to collect and disseminate vulnerability advisories, obtain and test software patches, and track patch implementation. These procedures will remain in effect until this "ideal" process can be implemented. The Department recognizes that preliminary efforts are necessary to position the Department to implement such a process, including:

- Obtain agreement from all Departmental elements involved to follow the process.
- Establish criteria for what constitutes an incident advisory as a Significant Event within Commerce.
- Development and maintenance of a hierarchical significant event call roster. Uppermost would be a DOC Significant Event Action Alert call roster that would be maintained by the DOC CIRT and consist of one Operating Unit Significant Incident Contact person for each operating unit. This Contact would in turn maintain a call roster of system owners, system administrators, or others as appropriate to the operating unit's system environment.
- Determine the method, or methods, of contact – pager, e-mail, fax – that are appropriate in times of emergency.
- Establish operating unit and DOC CIRT procedures, including roles and responsibilities, to implement the process within all operating units.
- Finalize the Department's use of the Patch Authentication and Dissemination Capability (PADC) through the Federal Computer Incident Response Center (FedCIRC). This would include establishing all system profiles and sub-accounts within the Department's PADC database.
- Establish 24x7 coverage for the DOC CIRT. Opportunities exist for cost-sharing if this coverage will extend to notification beyond the Operating Unit Significant Incident Contact.

Department of Commerce
Significant IT Security Event Coordination and Communication Process

Purpose

The occurrence of significant computer security events that affect systems within the federal government requires a process for timely, coordinated communication and specific action by Department of Commerce (DOC) personnel involved in computer incident response functions. A "Significant Event" is one which the Federal Computer Incident Response Center (FedCIRC) and the Office of Management and Budget (OMB) have determined to be of significant impact to the federal government. The process described below provides an organized, managed flow of initial personnel notifications within the Department, actions to be taken and time frames for the actions, and confirmation responses that appropriate actions are complete.

Scope

This is an activity coordination and communication process intended to supplement an operating unit's existing procedures for patch management and incident response. This process will be followed by personnel involved in computer security incident response, including:

- Office of the Department's Chief Information Officer (CIO), to include the Critical Infrastructure Program Manager (CIPM) and the DOC Computer Incident Response Team (CIRT); and
- Operating Unit Significant Event Contacts who may be CIOs, IT Security Officers, and formal CIRTs within DOC that support some operating units.

Process

Details of the process steps follow, and they are depicted graphically in attachment 1. Leading up to a Significant Event, all personnel on the FedCIRC mailing list receive incident advisories from the Federal Computer Incident Response Center (FedCIRC) and other sources on a regular basis, and each operating unit must have procedures documented and functioning to handle all these advisories. FedCIRC advisories will be followed by notification, from the Patch Authentication and Dissemination Capability (PADC) vendor to the CIPM (also the account manager for the Department's PADC agreement with FedCIRC) that patches are available and have been authenticated.

Event (E)	The issuance of a data call from the Federal Computer Incident Response Center (FedCIRC), OMB, or other external authority triggers a Significant Event. The DOC CIO or the CIPM receives such data calls from external entities.
E + 2 hrs	Within 1 hour of issuance of the data call, CIPM notifies the DOC Computer Incident Response Team (CIRT), staffed 24x7, of the Significant Event data call. The DOC CIRT begins work to enhance available FedCIRC advisories and to develop a DOC Significant IT Event Action Alert. Enhancement includes researching all available data on the event and developing steps for preventing event from entering DOC IT infrastructure, restricting spread of event within DOC, and to eradicate event from affected DOC systems. The DOC CIRT will have the enhanced alert ready for distribution within 2 hours of the data call issuance.

E + 2 hrs — The CIPM will query the PADC database to determine the DOC IT systems potentially affected by the event. Within 2 hours of the data call issuance, the CIPM provides the DOC CIRT with the names of DOC operating units that have affected (unpatched) systems.

E + 2 hrs — Upon notification from the CIPM of the operating units and systems affected, the DOC CIRT issues the enhanced Significant Event Action Alert/data call to the affected Operating Unit Significant Event Contacts. The alert also contains a request that Contacts update their respective PADC profiles and notify the DOC CIRT upon completion of corrective actions. This notification is issued within 2 hours of the data call issuance.

E + 4 hrs — Upon receipt of the DOC Significant Event Action Alert/data call from the DOC CIRT, the Operating Unit Significant Event Contact notifies its formal CIRT (if applicable and other than the DOC CIRT), owners of affected systems, and system administrators according to the operating unit's call roster. In addition, within 4 hours of the data call issuance, the Contact accesses the PADC database, reviews affected system profiles, and downloads authenticated patches for the system administrators (or assists the system administrators to download patches from PADC or directly from the software vendor).

E + 12 hrs — The corrective action implementer (e.g., the system administrator) obtains the authenticated patch from PADC or the software vendor. The implementer tests the patch on a development server or testbed, and installs the validated patch, and works with the DOC CIRT if difficulties arise with patch installation. Within 12 hours of the data call issuance, the implementer notifies the Operating Unit Significant Event Contact that corrective actions have been completed.

E + 16 hrs — Upon notification from the implementer that the patches have been tested and installed, the Operating Unit Significant Event Contact updates the PADC database for the affected systems and notifies the DOC CIRT that these actions are completed within 16 hours of the data call issuance.

E + 20 hrs — Upon notification from the Operating Unit Significant Event Contact that the corrective actions are complete and the PADC database has been updated, the DOC CIRT performs scans as necessary to validate the effectiveness of the patch installation, and works with the operating unit Contact to resolve discrepancies. Within 20 hours of the data call issuance, the DOC CIRT notifies the CIPM that corrective actions are complete and PADC is updated.

E + 24 hrs — Upon notification from the DOC CIRT that corrective actions are complete and validated, the CIPM confirms information in the PADC database and works with the Operating Unit Significant Event Contact to resolve discrepancies. Within 24 hours of the data call issuance, the CIPM can provide status updates to the DOC CIO and other external authorities as necessary.

Graphic Flow of DOC Significant Event Coordination and Communication Process